

Title	代数体の絶対ガロア群について (代数的整数論)
Author(s)	小松, 啓一
Citation	数理解析研究所講究録 (1975), 230: 13-25
Issue Date	1975-03
URL	http://hdl.handle.net/2433/105439
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

代数体の絶対ガロア群について

東京工大 理学部 小松啓一

標数 0 の体 F に対して、 \bar{F} によって F の代数的閉包、 G_F によって F の絶対ガロア群、即ち F と \bar{F} の間の位相的ガロア群をあらわす。この小論では絶対ガロア群どうしの同型は位相群としての同型を意味する。 \mathbb{Q} を有理数体、 $\mathcal{K}_1, \mathcal{K}_2$ を有限次代数体、即ち \mathbb{Q} の有限次拡大体とし、さらに次のような記号を用いる。

$\zeta_{\mathcal{K}_i}(s)$; \mathcal{K}_i の zeta 関数 $C(\mathcal{K}_i)$; \mathcal{K}_i のイデアル類群

h_i ; \mathcal{K}_i の類数 R_i ; \mathcal{K}_i の regulator

D_i ; \mathcal{K}_i の判別式 \mathcal{K}_{iA}^\times ; \mathcal{K}_i のイデール群

ただし $i = 1, 2$ である。この小論では次の定理の証明を目標とする。

定理 1. 有限次代数体 $\mathcal{K}_1, \mathcal{K}_2$ について、それらの絶対ガロア群を $G_{\mathcal{K}_1}, G_{\mathcal{K}_2}$ とする。このとき、 $G_{\mathcal{K}_1} \cong G_{\mathcal{K}_2}$ ならば $\zeta_{\mathcal{K}_1}(s) = \zeta_{\mathcal{K}_2}(s)$, $C(\mathcal{K}_1) \cong C(\mathcal{K}_2)$, $R_1 = R_2$, $D_1 = D_2$, $\mathcal{K}_{1A}^\times \cong \mathcal{K}_{2A}^\times$ となる。

定理 2. 有限次代数体 $\mathcal{L}_1, \mathcal{L}_2$ で $\mathcal{L}_{\mathcal{L}_1}(\mathcal{L}) = \mathcal{L}_{\mathcal{L}_2}(\mathcal{L})$ 且 $G_{\mathcal{L}_1} \neq G_{\mathcal{L}_2}$ となるものが存在する。

さてここで次の補題を引用する。

補題 1. ([2] の 363 ページ参照) L/\mathbb{Q} を有限次ガロア拡大 $\mathcal{L}_1, \mathcal{L}_2$ を L の部分体. $G = \text{Gal}(L/\mathbb{Q})$. $H_i = \text{Gal}(L/\mathcal{L}_i)$ とし. $\sigma \in G$ に対して $C(\sigma) = \{\tau \in G \mid \tau\sigma = \sigma\tau\}$ とする. このとき次は互いに同値である.

$$(i) \mathcal{L}_{\mathcal{L}_1}(\mathcal{L}) = \mathcal{L}_{\mathcal{L}_2}(\mathcal{L})$$

$$(ii) \forall \sigma \in G \text{ に対して } \text{card}(C(\sigma) \cap H_1) = \text{card}(C(\sigma) \cap H_2)$$

($\text{card}(C(\sigma) \cap H_i)$ は $C(\sigma) \cap H_i$ の元の個数をあらわす.)

系 1. 記号は補題 1 のままとする. \mathcal{L}_1/\mathbb{Q} が有限次ガロア拡大で, $\mathcal{L}_{\mathcal{L}_1}(\mathcal{L}) = \mathcal{L}_{\mathcal{L}_2}(\mathcal{L})$ ならば $\mathcal{L}_1 = \mathcal{L}_2$ となる。

証明. H_i は G の正規部分群だから $\sigma \in G$ に対して, $C(\sigma) \cap H_i$ は $C(\sigma)$ の元または空集合である. (ii) より $C(\sigma) \cap H_1 = C(\sigma) \Leftrightarrow C(\sigma) \cap H_2 = C(\sigma)$ 又, $C(\sigma) \cap H_1$ が空集合 $\Leftrightarrow C(\sigma) \cap H_2$ が空集合. よって $H_1 = H_2$. 即ち $\mathcal{L}_1 = \mathcal{L}_2$.

系 2. 記号は補題 1 のままとする. M_i を \mathcal{L}_i に含まれる \mathbb{Q} の最大のがロア拡大とする. ($i=1, 2$) このとき $\mathcal{L}_{\mathcal{L}_1}(\mathcal{L}) = \mathcal{L}_{\mathcal{L}_2}(\mathcal{L})$ ならば $M_1 = M_2$ となる。

証明. G の中で $\bigcup_{\sigma \in G} \sigma^{-1} H_i \sigma$ によって生成される部分群を $\langle \bigcup_{\sigma \in G} \sigma^{-1} H_i \sigma \rangle$ とすれば, $\text{Gal}(L/M_i) = \langle \bigcup_{\sigma \in G} \sigma^{-1} H_i \sigma \rangle$ となる. (ii)

より $\bigcup_{\sigma \in G} \sigma^{-1} H_1 \sigma = \bigcup_{\sigma \in G} \sigma^{-1} H_2 \sigma$ となるから $M_1 = M_2$ を得る。

体 F に対して μ_F によって、 F に含まれる 1 のべき根全体をあらわす。

補題 2. r_1, r_2 をそれぞれ \mathcal{L}_1 の実素点, 複素素点の個数とし、 r'_1, r'_2 をそれぞれ \mathcal{L}_2 の実素点, 複素素点の個数とする。このとき、 $\zeta_{\mathcal{L}_1}(s) = \zeta_{\mathcal{L}_2}(s)$ ならば $r_1 = r'_1, r_2 = r'_2, D_1 = D_2, f_1 R_1 = f_2 R_2$ となる。

証明. $\zeta_{\mathcal{L}_1}(s)$ は $s = -1$ で r_2 位の零点をもち、 $s = -2$ で $r_1 + r_2$ 位の零点をもつ。よって $\zeta_{\mathcal{L}_1}(s) = \zeta_{\mathcal{L}_2}(s)$ より $r_1 = r'_1, r_2 = r'_2$ となる。

$$Z_{\mathcal{L}_1}(s) = (\pi^{-\frac{s}{2}} \Gamma(\frac{s}{2}))^{r_1} ((2\pi)^{1-s} \Gamma(s))^{r_2} \zeta_{\mathcal{L}_1}(s)$$

$$Z_{\mathcal{L}_2}(s) = (\pi^{-\frac{s}{2}} \Gamma(\frac{s}{2}))^{r'_1} ((2\pi)^{1-s} \Gamma(s))^{r'_2} \zeta_{\mathcal{L}_2}(s)$$

と置く。このとき $Z_{\mathcal{L}_1}(s) = Z_{\mathcal{L}_2}(s)$ となる。 M_1, M_2 を補題 1 の系 2 のようにとる。 $\mu_{\mathcal{L}_i} = \mu_{M_i}$ 且つ $M_1 = M_2$ より $\mu_{\mathcal{L}_1} = \mu_{\mathcal{L}_2}$ となる。さらに a_i を $\mu_{\mathcal{L}_i}$ の元の個数とすれば $a_1 = a_2$ となる。よく知られているように、

$$\lim_{s \rightarrow 0} s Z_{\mathcal{L}_1}(s) = - \frac{2^{r_1} (2\pi)^{r_2} f_1 R_1}{a_1}$$

$$\lim_{s \rightarrow 0} s Z_{\mathcal{L}_2}(s) = - \frac{2^{r'_1} (2\pi)^{r'_2} f_2 R_2}{a_2} \quad \text{となる。} \quad ([9] \text{ の } 129$$

ページ参照) $r_1 = r'_1, r_2 = r'_2, a_1 = a_2$ より $f_1 R_1 = f_2 R_2$ を得る。さらに

$$\lim_{\alpha \rightarrow 1} (\alpha - 1) Z_{R_1}(\alpha) = |D_1|^{-\frac{1}{2}} \frac{2^{r_1} (2\pi)^{r_1} R_1}{a_1}$$

$$\lim_{\alpha \rightarrow 1} (\alpha - 1) Z_{R_2}(\alpha) = |D_2|^{-\frac{1}{2}} \frac{2^{r_2} (2\pi)^{r_2} R_2}{a_2}$$

となる事が知られている。([9] の 129 ページ参照)

よって $|D_1| = |D_2|$ となり、 D_1 の符号は $(-1)^{r_1}$ 、 D_2 の符号は $(-1)^{r_2}$ より、 $D_1 = D_2$ を得る。(証明終り)

補題 1, 系 1, 系 2, 補題 2 から $\zeta_{R_1}(\alpha) = \zeta_{R_2}(\alpha)$ ならば、

$R_1 \cong R_2$ が成立するのでもないかという問題が考えられるか
それに対しては次のような Gassmann による反例がある ([3]
参照) 補題 1 の記号をもちいて、 $\text{Gal}(L/\mathbb{Q}) = S_6$, $H_1 = \{1,$
 $(1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$, $H_2 = \{1, (1, 2)(3, 4), (1, 2)(5, 6), (3, 4)(5, 6)\}$
(ただし S_6 は 6 次対称群、 (ij) は互換である。) このとき $H_1,$
 H_2 は補題 1 の (ii) の条件を満足するか、 S_6 の中で共役でない。

\mathbb{Q} の代数的閉包 $\overline{\mathbb{Q}}$ の非アルキメデス的附値を \bar{v} とし、 \bar{v} の
 \mathbb{Q} への制限が有理素数 p に対応しているとする。 R/\mathbb{Q} を有限
次拡大とし、 \bar{v} の R への制限を v とする。 R の v による完備
化を R_v とすれば、 R_v 中の \mathbb{Q} の位相的閉包は p -進体 \mathbb{Q}_p と
なる。さらに R_v/\mathbb{Q}_p は有限次である。

$D_R(\bar{v}) = \{\sigma \in G_R \mid \bar{v}(x^\sigma) = \bar{v}(x) \quad \forall x \in \overline{\mathbb{Q}}\}$ と置く。 $\overline{\mathbb{Q}}$ を R_v
の中へ適当に埋蔵してやれば、

$$(1) \quad G_{R_v} \cong G_{\overline{\mathbb{Q}} \cap R_v} = D_R(\bar{v}) \quad \text{を得る。}$$

よって $D_{\mathbb{R}}(\bar{v})$ は $G_{\mathbb{Q}_p}$ の開部分群と位相群として同型になる。
 $G_{\mathbb{Q}}$ の元 σ に対して、 \bar{v}^σ を $\bar{v}^\sigma(x) = \bar{v}(x^\sigma)$ $\forall x \in \bar{\mathbb{Q}}$ によって定義する。 \bar{v} の $\bar{\mathbb{Q}}$ への延長を \bar{v} とすれば、 $G_{\mathbb{R}}$ の元 τ で $\bar{v}' = \bar{v}^\tau$ となるものが存在する事が知られている。よって

$$(2) \quad D_{\mathbb{R}}(\bar{v}') = \tau D_{\mathbb{R}}(\bar{v}) \tau^{-1} \quad \text{となる。}$$

定義 G を *pro-finite group* とし、 p を有理素数とする。
 G が $G_{\mathbb{Q}_p}$ の開部分群と位相群として同型なとき、 G は L_p -group
 といわれる。 ([7] 参照)

ここで次の補題を引用する。

補題 3. ([7] 参照) \mathbb{R}/\mathbb{Q} を有限次拡大、 K/\mathbb{R} を代数拡大とする。このとき次は同値である。 (p は有理素数とする。)

- (i) G_K は $G_{\mathbb{R}}$ の (包含関係についての) maximal L_p -group.
- (ii) p の上にある $\bar{\mathbb{Q}}$ の valuation (附値) \bar{v} で $D_{\mathbb{R}}(\bar{v}) = G_K$ となるものがある。

上のような \bar{v} は同値な附値を除いて一意的にきまる。

\mathbb{R}_i/\mathbb{Q} を有限次拡大、 $\mathcal{O}_{\mathbb{R}_i}$ を \mathbb{R}_i の整数環、 $\text{Spec}(\mathcal{O}_{\mathbb{R}_i})$ を $\mathcal{O}_{\mathbb{R}_i}$ の素イデアル全体とする。 ($i=1, 2$) $G_{\mathbb{R}_1} \cong G_{\mathbb{R}_2}$ とし、 $G_{\mathbb{R}_1}$ から $G_{\mathbb{R}_2}$ の上への同型写像を λ とする。このとき *Kaukisch* は次のようにして、 $\text{Spec}(\mathcal{O}_{\mathbb{R}_1})$ から $\text{Spec}(\mathcal{O}_{\mathbb{R}_2})$ への bijection $\Phi_{\lambda, \mathbb{R}_1}$ を導いた。 ([7] 参照) $\mathfrak{p}_1 \in \text{Spec}(\mathcal{O}_{\mathbb{R}_1})$ とし、 \mathfrak{p}_1 は有理素数 p

の上にあるとする。即ち \mathfrak{p}_1 は ideal $\rho \mathcal{O}_{K_1}$ を割り切る。 \mathfrak{p}_1 に対応する \mathcal{O}_{K_1} の附値を v_1 とし、 v_1 の $\overline{\mathbb{Q}}$ への延長を \overline{v}_1 とする。補題 3 より $D_{K_1}(\overline{v}_1)$ は G_{K_1} の maximal L_p -group である。よって $\lambda(D_{K_1}(\overline{v}_1))$ は G_{K_2} の maximal L_p -group となり、補題 3 より ρ の上にある $\overline{\mathbb{Q}}$ の附値 \overline{v}_2 で $D_{K_2}(\overline{v}_2) = \lambda(D_{K_1}(\overline{v}_1))$ となるものが存在して、同値なものを除いて一意にきまる。 \overline{v}_2 の \mathcal{O}_{K_2} への制限に対応する素イデアルを $\mathfrak{p}_{\lambda, K_2}(\mathfrak{p}_1)$ と定義する。 $\mathfrak{p}_{\lambda, K_2}$ が well-defined なる事を示す。 v_1 の $\overline{\mathbb{Q}}$ への延長のしかたに無関係に $\mathfrak{p}_{\lambda, K_2}$ がきまる事をいえばよい。 v_1 の $\overline{\mathbb{Q}}$ への延長を \overline{v}_1' とする。(2) より G_{K_1} の元 τ_1 で $D_{K_1}(\overline{v}_1') = \tau_1 D_{K_1}(\overline{v}_1) \tau_1^{-1}$ となるものがある事かわかる。よって $\lambda(D_{K_1}(\overline{v}_1')) = \lambda(\tau_1) \lambda(D_{K_1}(\overline{v}_1)) \lambda(\tau_1)^{-1} = D_{K_2}(\overline{v}_2^{\lambda(\tau_1)})$ となる。 $\lambda(\tau_1) \in G_{K_2}$ より $\overline{v}_2^{\lambda(\tau_1)}$ の \mathcal{O}_{K_2} への制限と \overline{v}_2 の \mathcal{O}_{K_2} への制限は一致する。よって $\mathfrak{p}_{\lambda, K_2}$ は well-defined。 λ の逆写像 $\lambda^{-1}; G_{K_2} \cong G_{K_1}$ に対して $\mathfrak{p}_{\lambda^{-1}, K_2}$ を考えれば、

$$\mathfrak{p}_{\lambda, K_2} \circ \mathfrak{p}_{\lambda^{-1}, K_1} = \text{Id}_{\text{Spec}(\mathcal{O}_{K_1})}$$

$$\mathfrak{p}_{\lambda^{-1}, K_1} \circ \mathfrak{p}_{\lambda, K_2} = \text{Id}_{\text{Spec}(\mathcal{O}_{K_2})} \quad \text{となる事は簡単にわかる。}$$

従って $\mathfrak{p}_{\lambda, K_2}; \text{Spec}(\mathcal{O}_{K_1}) \rightarrow \text{Spec}(\mathcal{O}_{K_2})$ は bijection。 \mathfrak{p}_1 に対応する \mathcal{O}_{K_1} の附値 v_1 による \mathcal{O}_{K_1} の完備化を $\mathcal{O}_{K_1, \mathfrak{p}_1}$ と記せば、(1) より

$$(3) \quad G_{K_1, \mathfrak{p}_1} \cong G_{K_2, \mathfrak{p}_{\lambda, K_2}(\mathfrak{p}_1)} \quad \forall \mathfrak{p}_1 \in \text{Spec}(\mathcal{O}_{K_1}) \quad \text{を得る。}$$

K_1/\mathbb{Q} を有限次拡大とすれば、 G_{K_1} は G_{K_1} の開部分群だから $\lambda(G_{K_1})$ は G_{K_2} の開部分群となり、 \mathcal{O}_{K_2} の有限次拡大 K_2 で $\lambda(G_{K_1}) = G_{K_2}$

となるものが存在する事がわかる。 λ の G_{K_1} への制限 $\lambda|_{G_{K_1}}$ に対して Kummer の bijection $\Phi_{\lambda|_{G_{K_1}}, K_1}: \text{Spec}(\mathcal{O}_{K_1}) \rightarrow \text{Spec}(\mathcal{O}_{K_2})$ を考えられるが、これを Φ_{λ, K_1} と略記する。 $\mathfrak{p}_1 \in \text{Spec}(\mathcal{O}_{K_1})$ に対して \mathfrak{p}_1 の $\mathcal{O}_{K_1}/\mathbb{Q}$ における分岐指数を $e_{K_1}(\mathfrak{p}_1)$ であらわす。 $\text{Spec}(\mathcal{O}_{K_2})$, $\text{Spec}(\mathcal{O}_{K_1})$, $\text{Spec}(\mathcal{O}_{K_2})$ の元についても同様の記号をもちいる。

F_i/\mathbb{Q}_p を m_i 次拡大とし、 f_i を相対次数、 e_i を分岐指数、 μ_{F_i} の p -Sylow 群の位数を p^{a_i} とする。 ($i=1, 2$) (G_{F_i}, G_{F_i}) によって G_{F_i} の topological commutator group を表わす。 このとき局所類体論より次の事がわかる。

(4) $G_{F_i}^{\text{ab}} \cong G_{F_i} / (G_{F_i}, G_{F_i}) \cong \prod_{\ell} \mathbb{Z}_{\ell} \times \mathbb{Z}_p^{m_i} \times \mathbb{Z}/(p^{f_i}-1)\mathbb{Z} \times \mathbb{Z}/p^{a_i}\mathbb{Z}$
 (ただし、 \prod_{ℓ} はすべての素数 ℓ をわたり、 \mathbb{Z} は有理整数環 \mathbb{Z}_{ℓ} は ℓ -adic integer ring をあらわす。)

さらに F_i の乗法群を F_i^{\times} とすれば

(5) $F_i^{\times} \cong \mathbb{Z} \times \mathbb{Z}_p^{m_i} \times \mathbb{Z}/(p^{f_i}-1)\mathbb{Z} \times \mathbb{Z}/p^{a_i}\mathbb{Z}$ となる事が知られている。

補題 4. ([5]参照) 記号は上のとうりとする。

$$G_{F_1} \cong G_{F_2} \Rightarrow F_1^{\times} \cong F_2^{\times}, \quad e_1 = e_2, \quad p^{f_1} = p^{f_2}$$

証明. $G_{F_1} \cong G_{F_2}$ より $G_{F_1}^{\text{ab}} \cong G_{F_2}^{\text{ab}}$. よって (4) を用いれば、

$\prod_{\ell} \mathbb{Z}_{\ell} \times \mathbb{Z}_p^{m_1} \times \mathbb{Z}/(p^{f_1}-1)\mathbb{Z} \times \mathbb{Z}/p^{a_1}\mathbb{Z} \cong \prod_{\ell} \mathbb{Z}_{\ell} \times \mathbb{Z}_p^{m_2} \times \mathbb{Z}/(p^{f_2}-1)\mathbb{Z} \times \mathbb{Z}/p^{a_2}\mathbb{Z}$
 となる。 $G_{F_1}^{\text{ab}}$ と $G_{F_2}^{\text{ab}}$ の maximal torsion subgroup は互いに同型たから、 (6) $\mathbb{Z}/(p^{f_1}-1)\mathbb{Z} \times \mathbb{Z}/p^{a_1}\mathbb{Z} \cong \mathbb{Z}/(p^{f_2}-1)\mathbb{Z} \times \mathbb{Z}/p^{a_2}\mathbb{Z}$ を得る。

よって $p^{f_1} = p^{f_2}$ となる。 $G_{F_1}^{ab}$ と $G_{F_2}^{ab}$ の p -sylow 群は互いに同型だから $\mathbb{Z}_p^{m_1+1} \times \mathbb{Z}/p^{f_1}\mathbb{Z} \cong \mathbb{Z}_p^{m_2+1} \times \mathbb{Z}/p^{f_2}\mathbb{Z}$ となる。よって $m_1 = m_2$ となり、 $m_i = e_i f_i$ より $e_1 = e_2$ を得る。(5), (6) および $m_1 = m_2$ より $F_1^* \cong F_2^*$ を得る。(証明終り)

補題5. ([5]参照) \mathbb{R}_1/\mathbb{Q} , \mathbb{R}_2/\mathbb{Q} , K_1/\mathbb{R}_1 を有限次拡大とし、 $G_{\mathbb{R}_1} \cong G_{\mathbb{R}_2}$ とする。 $G_{\mathbb{R}_1}$ から $G_{\mathbb{R}_2}$ の上への同型写像を λ とし、 $\lambda(G_{K_1}) = G_{K_2}$ とする。 $\mathfrak{p} \in \text{Spec}(\mathcal{O}_{\mathbb{R}_1})$, $\mathfrak{P} \in \text{Spec}(\mathcal{O}_{K_1})$ とする。このとき次が成立する。

$$(i) e_{\mathbb{R}_1}(\mathfrak{p}) = e_{\mathbb{R}_2}(\lambda_{\lambda, \mathbb{R}_1}(\mathfrak{p})), \quad e_{K_1}(\mathfrak{P}) = e_{K_2}(\lambda_{\lambda, K_1}(\mathfrak{P}))$$

$$N_{\mathbb{R}_1/\mathbb{Q}}(\mathfrak{p}) = N_{\mathbb{R}_2/\mathbb{Q}}(\lambda_{\lambda, \mathbb{R}_1}(\mathfrak{p})), \quad N_{K_1/\mathbb{Q}}(\mathfrak{P}) = N_{K_2/\mathbb{Q}}(\lambda_{\lambda, K_1}(\mathfrak{P}))$$

(ただし $N_{\mathbb{R}_2/\mathbb{Q}}, N_{K_2/\mathbb{Q}}$ はイデアルの絶対ノルム)

(ii) \mathfrak{P} が \mathfrak{p} の上にある。 $\iff \lambda_{\lambda, K_1}(\mathfrak{P})$ は $\lambda_{\lambda, \mathbb{R}_1}(\mathfrak{p})$ の上にある。

$$(iii) \mathbb{R}_{1, \mathfrak{p}}^* \cong \mathbb{R}_{2, \lambda_{\lambda, \mathbb{R}_1}(\mathfrak{p})}^*, \quad K_{1, \mathfrak{P}}^* \cong K_{2, \lambda_{\lambda, K_1}(\mathfrak{P})}^*$$

証明. $\mathfrak{p} \in \text{Spec}(\mathcal{O}_{\mathbb{R}_1})$ とし、 \mathfrak{p} は有理素数 p の上にあるとする。

(i) の証明. \mathfrak{p} の \mathbb{R}_1/\mathbb{Q} における分岐指数 $e_{\mathbb{R}_1}(\mathfrak{p})$ は $\mathbb{R}_{1, \mathfrak{p}}/\mathbb{Q}_p$ の分岐指数に等しく、 $\mathbb{R}_{1, \mathfrak{p}}/\mathbb{Q}_p$ の相対次数を f とすれば、 $N_{\mathbb{R}_1/\mathbb{Q}}(\mathfrak{p}) = p^f$ となる。よって(3)および補題4から $e_{\mathbb{R}_1}(\mathfrak{p}) = e_{\mathbb{R}_2}(\lambda_{\lambda, \mathbb{R}_1}(\mathfrak{p}))$, $N_{\mathbb{R}_1/\mathbb{Q}}(\mathfrak{p}) = N_{\mathbb{R}_2/\mathbb{Q}}(\lambda_{\lambda, \mathbb{R}_1}(\mathfrak{p}))$ が成立する。 $\mathfrak{P} \in \text{Spec}(\mathcal{O}_{K_1})$ についても同様である。

(ii) の証明. \mathfrak{P} が \mathfrak{p} の上にあるとする。 \mathfrak{P} に対応する K_1 の附

値の $\bar{\mathbb{Q}}$ への延長を $\bar{\sigma}_1$ とする。 $\bar{\sigma}_1$ の $\bar{\mathcal{L}}_1$ への制限は $\bar{\rho}$ に対応する $\bar{\mathcal{L}}_1$ の附値である。補題3. および $\bar{\sigma}_{\lambda, \bar{\mathcal{L}}_1}$ の定義の仕方を見れば $\lambda(D_{\bar{\mathcal{L}}_1}(\bar{\sigma}_1)) = D_{\bar{\mathcal{L}}_2}(\bar{\sigma}_2)$ となる $\bar{\mathbb{Q}}$ の附値 $\bar{\sigma}_2$ で ρ の上にあるものが存在する事がわかる。 $D_{K_1}(\bar{\sigma}_1) = D_{\bar{\mathcal{L}}_1}(\bar{\sigma}_1) \cap G_{K_1}$, $\lambda(D_{K_1}(\bar{\sigma}_1)) = D_{\bar{\mathcal{L}}_2}(\bar{\sigma}_2) \cap G_{K_2} = D_{K_2}(\bar{\sigma}_2)$ よって $\bar{\sigma}_{\lambda, K_1}(\bar{\rho})$ は $\bar{\sigma}_2$ の K_2 への制限に対応する K_2 の素イデアル $\bar{\sigma}_{\lambda, \bar{\mathcal{L}}_2}(\bar{\rho})$ は $\bar{\sigma}_2$ の $\bar{\mathcal{L}}_2$ への制限に対応する $\bar{\mathcal{L}}_2$ の素イデアル。よって $\bar{\sigma}_{\lambda, K_1}(\bar{\rho})$ は $\bar{\sigma}_{\lambda, \bar{\mathcal{L}}_2}(\bar{\rho})$ の上にある。逆は $\bar{\sigma}_{\lambda', K_2}$, $\bar{\sigma}_{\lambda', \bar{\mathcal{L}}_2}$ を考える事によりわかる。

(iii) の証明. (3) および補題4 から明らか。(証明終り)

上の補題5は[7]の Lemma 3 の精密化である。

K_1 を $\bar{\mathcal{L}}_1$ の絶対類体。即ち最大不分岐 abel 拡大とする。このとき $\text{Gal}(K_1/\bar{\mathcal{L}}_1) \cong C(\bar{\mathcal{L}}_1)$ なる事が知られている。補題5の仮定と記号のもとで、補題5の (i), (ii) から K_2 は $\bar{\mathcal{L}}_2$ の不分岐拡大なる事がわかる。さらに $\text{Gal}(K_1/\bar{\mathcal{L}}_1) \cong G_{\bar{\mathcal{L}}_1}/G_{K_1} \cong G_{\bar{\mathcal{L}}_2}/G_{K_2} \cong \text{Gal}(K_2/\bar{\mathcal{L}}_2)$ より K_2 は $\bar{\mathcal{L}}_2$ の abel 拡大なる事がわかる。よって K'_2 を $\bar{\mathcal{L}}_2$ の絶対類体とすれば $K'_2 \supset K_2$ となる。 $\lambda^{-1}(G_{K'_2}) = G_{K'_1}$ とすれば、 K'_1 は $\bar{\mathcal{L}}_1$ の不分岐 abel 拡大となり、 $K_1 \supset K'_1$ となる。 $G_{K_2} = \lambda(G_{K_1}) \subset \lambda(G_{K'_1}) = G_{K'_2}$ より $K_2 \supset K'_2$ 。よって $K_2 = K'_2$ 。即ち K_2 は $\bar{\mathcal{L}}_2$ の絶対類体となる。故に $C(\bar{\mathcal{L}}_1) \cong C(\bar{\mathcal{L}}_2)$ なる事がわかる。以上をまとめて次の系を得る。

系 $\bar{\mathcal{L}}_1/\mathbb{Q}$, $\bar{\mathcal{L}}_2/\mathbb{Q}$ を有限次拡大とする。このとき $G_{\bar{\mathcal{L}}_1} \cong G_{\bar{\mathcal{L}}_2}$ な

らば $C(\mathbb{R}_1) \cong C(\mathbb{R}_2)$ となる。

ここまてくれば、定理 1 の証明は容易である。

定理 1 の証明. $G_{\mathbb{R}_1}$ から $G_{\mathbb{R}_2}$ の上への同型写像を λ とする。

複素数 Δ について、補題 5 より、

$$\zeta_{\mathbb{R}_1}(\Delta) = \prod_{\rho \in \text{Spec}(\mathcal{O}_{\mathbb{R}_1})} (1 - N_{\mathbb{R}_1/\mathbb{Q}}(\rho)^{-\Delta})^{-1} = \prod_{\rho \in \text{Spec}(\mathcal{O}_{\mathbb{R}_1})} (1 - N_{\mathbb{R}_2/\mathbb{Q}}(\lambda_{\lambda, \mathbb{R}_1}(\rho))^{-\Delta})^{-1} = \zeta_{\mathbb{R}_2}(\Delta)$$

($\text{Re } \Delta > 1$) よって補題 2 より $D_1 = D_2$, $R_1 R_1 = R_2 R_2$. 補題 5 の系から $C(\mathbb{R}_1) \cong C(\mathbb{R}_2)$ より $R_1 = R_2$. よって $R_1 = R_2$. 補題 5 の (iii) および補題 2 の $r_1 = r_1'$, $r_2 = r_2'$ より $\mathbb{R}_{1A}^\times \cong \mathbb{R}_{2A}^\times$ がわかる。

(証明終り)

補題 6. \mathbb{R}_1/\mathbb{Q} , \mathbb{R}_2/\mathbb{Q} を有限次拡大, L によって \mathbb{R}_1 を含む \mathbb{Q} の有限次ガロア拡大を表わす。 $G_{\mathbb{R}_1} \cong G_{\mathbb{R}_2}$ ならば $L \supset \mathbb{R}_2$ 且つ $\text{Gal}(L/\mathbb{R}_1) \cong \text{Gal}(L/\mathbb{R}_2)$ となる。

証明. $G_{\mathbb{R}_1}$ から $G_{\mathbb{R}_2}$ の上への同型写像を λ とする。 $\lambda(G_L)$ は $G_{\mathbb{R}_2}$ の開部分群だから \mathbb{R}_2 の有限次拡大 L' で $\lambda(G_L) = G_{L'}$ となるものがある。定理 1 より $\zeta_L(\Delta) = \zeta_{L'}(\Delta)$ だから補題 1 の系 1 より $L = L'$ となり、 $L \supset \mathbb{R}_2$ を得る。 $\text{Gal}(L/\mathbb{R}_1) \cong G_{\mathbb{R}_1}/G_L$ 且つ λ により $G_{\mathbb{R}_1}/G_L$ から $G_{\mathbb{R}_2}/G_L$ の上への同型が導かれるから $\text{Gal}(L/\mathbb{R}_1) \cong \text{Gal}(L/\mathbb{R}_2)$ 。

(証明終り)

定理 2 を示すためには、補題 6 から、補題 1 の (ii) の条件をみたす H_1, H_2 で $H_1 \cong H_2$ となるものをみつければよい事になった。 p を奇素数、 H_1 を位数 p^3 の基本 abel 群。即ち $H_1 \cong (\mathbb{Z}/p\mathbb{Z})^3$ 。

H_2 を位数 p^3 の非可換群で単位元 e 以外の元の位数はすべて p なるものとする。(その存在は[1]の187ページ例題 8.2) S_{p^3} を $\{1, 2, \dots, p^3\}$ の置換全体のなす群とし、 H_2 の元をあらべて a_1, \dots, a_{p^3} とする。 H_2 の元 a に対して、 S_{p^3} の元 σ で

$$\begin{pmatrix} a_1 & a_2 & \dots & a_{p^3} \\ a_1 a & a_2 a & \dots & a_{p^3} a \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_{p^3} \\ a_{\sigma(1)} & a_{\sigma(2)} & \dots & a_{\sigma(p^3)} \end{pmatrix}$$

となるものを対応させる。これによって H_2 を S_{p^3} にうめこんだものを再び H_2 と記す。このとき次が成立する。

補題 7. H_1, H_2, S_{p^3} を上のようにとる。このとき

$\text{card}(C(\sigma) \cap H_1) = \text{card}(C(\sigma) \cap H_2)$ が S_{p^3} のすべての元 σ に対して成立する。

証明. H_2 の S_{p^3} への入れかたから、単位元 e 以外の H_2 のすべての元 τ は $\tau(j) \neq j$ ($j = 1, \dots, p^3$) さらに $\tau^p = e$ 。よって τ を互いに共通文字を含まない巡回置換の積に分解すれば、

$\tau = (j_{11} \dots j_{1p}) \dots (j_{p^2 1} \dots j_{p^2 p})$ というように長さ p の巡回置換

p^2 個の積となる。 S_{p^3} の2つの元が互いに共役であるための必要十分条件は両者の巡回因子分解の型が一致する事である。

したがって $H_1 \cup H_2$ の e 以外の元 τ_1, τ_2 は S_{p^3} の中で共役である。

よって $\text{card}(C(\tau) \cap H_1) = \text{card}(C(\tau) \cap H_2) = p^3 - 1$ $\tau \in H_1 \cup H_2$ $\tau \neq e$

$$\text{card}(C(e) \cap H_1) = \text{card}(C(e) \cap H_2) = 1$$

S_{p^3} の元 $\sigma \neq e$ について $C(\sigma) \cap H_1 = \emptyset \Leftrightarrow C(\sigma) \cap H_2 = \emptyset$

$$C(\alpha) \cap H_1 \neq \emptyset \Leftrightarrow C(\alpha) \cap H_2 \neq \emptyset \Leftrightarrow \text{card}(C(\alpha) \cap H_1) = \text{card}(C(\alpha) \cap H_2) = p^3 - 1$$

よってすべての元に対して $\text{card}(C(\alpha) \cap H_1) = \text{card}(C(\alpha) \cap H_2)$ 。ただし \emptyset は空集合を表す。(証明終り)

定理 2 の証明. よく知られているように S_{p^3} と同型なガロア群をもつ \mathbb{Q} のガロア拡大は存在する。それを L とし, $\text{Gal}(L/\mathbb{Q})$ から S_{p^3} の上への同型写像を φ とする。 S_{p^3} の部分群 H_1, H_2 を上のようにとり, $\varphi(\text{Gal}(L/\mathbb{Q}_i)) = H_i$ となるように L/\mathbb{Q} の中間体 \mathbb{Q}_i をとる。 H_1, H_2 は補題 1 の (ii) の条件を満足するから, $G_{\mathbb{Q}_1}(\alpha) = G_{\mathbb{Q}_2}(\alpha)$ となる。一方 $H_1 \neq H_2$ より $G_{\mathbb{Q}_1} \neq G_{\mathbb{Q}_2}$ (証明終り)

定理 1, 定理 2 から $G_{\mathbb{Q}_1}(\alpha) = G_{\mathbb{Q}_2}(\alpha)$ よりも $G_{\mathbb{Q}_1} \cong G_{\mathbb{Q}_2}$ の方が本当に強い条件である事がわかった。

文 献

- [1] 浅野啓三, 永尾汎, 群論, 岩波書店, (1965)
- [2] Cassels-Fröhlich, Algebraic Number Theory, Academic Press, London & New York (1967)
- [3] F. Gassmann, Bemerkungen zur vorstehenden Arbeit von Hurwitz, Math. Zeitsch. 25, 665-675 (1926)
- [4] T. Kanno, Automorphisms of the Galois group of the algebraic closure of the rational number field, Kodai Math. Sem. Report, 25, 446-448 (1973)

- [5] K. Komatsu, The Galois group of the algebraic closure of an algebraic number field, Kodai Math. Sem. Report, 26, 44-52 (1974)
- [6] S. Nakatsuchi, A note on Kronecker's "Randwertsatz", Journal of Math. of Kyoto University, 13, 129-137, (1972)
- [7] J. Neukirch, Kennzeichnung der p -adischen und der endlich algebraischen Zahlkörper, Inventiones Math., 6, 296-314 (1969)
- [8] ———, Kennzeichnung der endlich-algebraischen Zahlkörper durch die Galoisgruppe der maximal auflösbaren Erweiterung, J. Reine Angew. Math., 238, 135-197 (1969)
- [9] A. Weil, Basic Number Theory, Springer-Verlag (1967)